Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

July 16, 2004

Via Facsimile and Overnight Delivery

Mr. Donald S. Clark
Secretary
Federal Trade Commission
Room 159-H
500 Pennsylvania Avenue, NW
Washington, DC 20580

RE: CAN-SPAM Act Rulemaking

Dear Secretary Clark:

Microsoft submits these comments to assist the Commission in developing regulations to implement provisions of the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (the "CAN-SPAM Act" or "Act"). This letter is provided to assist the Commission with preparing its report to Congress, required by Section 11(1)(A) of the Act, setting forth a system for rewarding those who supply information about violations of the Act.

Microsoft believes that reward systems can be very helpful when implemented strategically and with the proper incentives. As outlined below, Microsoft supports the implementation of a program that offers a reward of not less than 20% of any civil penalty collected from spammers or $25,000, whichever is greater. Microsoft recommends offering this reward only in limited and tactically appropriate situations, in order to elicit insider information from knowledgeable participants in select spamming operations.

SYSTEM FOR REWARDING THOSE WHO SUPPLY INFORMATION ABOUT VIOLATIONS

The Act obligates the Commission to write a report setting forth a system by which a reward of not less than 20% of the total civil penalty collected for a violation of the Act is provided to "the first person that identifies the person in violation of the Act, and supplies information that leads to the successful collection of a civil penalty by the Commission." See Section 11(1). Microsoft believes that with a few modifications, such a reward program could become an effective element of the Commission's battle against spammers. Based on our experience both with spam investigations and with reward programs, we believe that any offer of reward should have a concrete and unconditional minimum of sufficient size to create the necessary incentives. Thus, we would propose

Microsoft Corporation is an equal opportunity employer.

consideration of a system that offers a reward of not less than 20% of any civil penalty collected from spammers or $25,000, whichever is greater. Likewise, we would recommend that rewards be offered only in connection with specific investigations of notable or high-profile spam campaigns.

A. STRUCTURING THE REWARD

We have found that an important component of a reward program is a clear, unambiguous, and certain reward. This certainty is necessary to motivate insiders or others with critical information about co-workers or associates to come forward. Likewise, the reward must be sufficiently large to induce insiders to provide information against professional or personal acquaintances. In our Anti-Virus Reward Program (see *www.microsoft.com/security/antivirus)*, we have found that a reward of $250,000 has provided a sufficient incentive for insiders and other informants to approach law enforcement with potential evidence of criminal virus propagation. For a number of reasons, Microsoft believes that the Commission should consider a reward of lesser magnitude for spammers. Most importantly, unlike viruses, the distribution of spam typically involves a loosely connected affiliation of business associates who are responsible for creating and sending the spam. In addition, the spam is typically part of a broader business campaign that involves the sale of goods or services. This broad network of businesses offers much greater opportunity for insiders who are willing to come forward with information. Based on our experience, Microsoft believes that a reward of $25,000 would be sufficient incentive to induce tipsters to come forward.

We observe that a reward tied to the collection of civil penalties from spammers, while intriguing, may not be definite enough to create a strong incentive to tipsters. Although the Act does provide for the imposition of civil penalties, it also gives great discretion to the Court in how large a penalty to impose. More importantly, there is a great gulf between the imposition of penalties and the collection of those penalties. In our experience, judgments against spammers are frequently uncollectible, and the ability to recover from any individual spammer is not particularly predictable at the outset of an investigation. In general, prosecution of spammers is not a money-making enterprise, as the costs of investigation and enforcement can often exceed recoverable assets. This lack of certainty suggests that a reward simply tied to the collection of penalties is too tentative and uncertain to motivate a good tipster.

To overcome this problem, we suggest that a reward should have an alternative fixed minimum component of sufficient size to create both the necessary certainty and motivation. An offered reward of either 20% of collected civil penalties ***or*** $25,000 provides both the certainty and incentive we would expect to create results.

B. CIRCUMSTANCES IN WHICH THE REWARD SHOULD BE OFFERED

We have also found that reward systems can be very effective when used sparingly for specific, identifiable and important cases. Surrounded by appropriate publicity, rewards directed at particular identifiable conduct or events can produce

astounding results. For example, the publicity surrounding our Anti-Virus Reward Program motivated an "insider" with information about the Sasser computer worm to provide critical and otherwise unattainable information that helped lead to an arrest. In a similar vein, the Commission may want to evaluate the possibility of implementing a program that publicizes a reward for tangible inside information that leads to the recovery of a civil judgment against the individual or entities behind a particular spam operation or series of spam campaigns.

Our experience is that an offer of reward can and does work to encourage disclosure of information held by persons with direct, personal knowledge of illegal operations – often current and former employees – whose evidence is both admissible and compelling. The tipsters who we find most valuable, and whose information is often unique and not otherwise obtainable, are those who have themselves indirectly or unwittingly participated in the spamming operations. Indeed, given that in many instances the Act predicates liability on proof of knowledge or willfulness,[1] the testimony of spamming insiders is precisely the type of inimitable evidence that is likely to make prosecution effective.[2] Because spam procurers frequently operate in loosely affiliated networks and hide behind layers of ever-shifting people, entities and technical resources, forensic and technical evidence will often not be sufficient to bring them to justice. Rather, direct, first-hand testimony from insiders themselves makes spam prosecutions most effective.

In our view, a reward system would work best for motivating insider informants to come forth in particular cases, rather than for encouraging the delivery of voluminous, relatively generic, and inadmissible reports on spammers. Based on our experience with such systems, we suggest that the Commission might wish to consider offering rewards only in connection with specific, important and high-profile investigations.

C. Considerations in the Implementation of a Ubiquitous Reward Program

The Act seemingly contemplates the prospect of offering a reward in every prosecution to "the first person that identifies the person in violation of the Act, and supplies information that leads to the successful collection of a civil penalty by the Commission." See Section 11(1). We have concerns that in practice a universal reward program, applied without direction or discretion, may be more likely to be disruptive than

---

[1] See, e.g., Section 5(b)(1)(liability for harvesting requires actual or imputed knowledge); Section 6(a)(1)(liability only with actual or imputed knowledge); Section 7(f)(9)(scienter required for civil liability); Section 7(f)(3)(C)(aggravated damages only if defendant acts "willfully and knowingly"); Section 7(g)(3)(C)(same).

[2] Before issuing rewards to insiders, it is important to determine the degree to which the insiders may have participated in the illegal operation and whether any such participation warrants exclusion from eligibility for a reward. As a general matter, a person who aids or abets in the commission or concealment of criminal spamming is properly excluded from a reward relating to that spam activity. See, e.g., 77 C.J.S. *Rewards* § 34.

helpful to the Commission's enforcement efforts. However, we believe that a more targeted and narrow approach could prove to be very effective.

As the Commission is well aware, there is already no shortage of spam-related leads worthy of investigation. The Commission, state and federal enforcement agencies, and most ISPs are already besieged with complaints about spam. E-mail subscribers, anti-spam advocates, and frustrated citizens currently create a robust community of private parties interested in stopping spam, and the leads generated by this community already constitute an overwhelming pool of available information. For example, Microsoft's MSN Hotmail system obtains many thousands of "junk mail reports" every day, and Microsoft collects for further investigation and analysis approximately a million e-mail messages each week. Likewise, the Commission and many state Attorneys General maintain web-based electronic interfaces by which consumers report spam in significant volume.

The challenge to enforcement agencies is not the creation of leads but, rather, is the sorting, sifting and selection of the most promising leads. The available set of leads already vastly exceeds the resources available to investigate them. Thus, there is no lack of candidates for enforcement efforts, and it is not particularly important to expand the pool of investigative targets through tips from spam recipients or anti-spam investigators.

Likewise, there is no shortage of leads purporting to tie a set of spam to a particular spammer or group of spammers. The anti-spam community is quite active in compiling examples of spam and identifying its purported source. A simple search of webpostings, or a review of the websites of anti-spam organizations, reveals a wealth of source material, data and investigative results attributing spam to particular known spamming operations. Anti-spam resources available on the internet include the Spamhaus ROKSO list (the Registry of Known Spam Operations), SPEWS (Spam Prevention Early Warning System), and N.A.N.-A.E., a USENET newsgroup which discusses email spamming. An amazing amount of research on many spam targets has already been compiled by these and other anti-spam activists.

In most cases, however, their purported identification of a particular spammer is based on supposition and inference, and not on legally admissible evidence. As we have found in our spam investigations, without subpoena power to follow the trail of a spammer, private parties are simply unable to compile the necessary evidence to link a spammer to a spam campaign. Lacking subpoena power, an anti-spam activist, no matter how well qualified and well intentioned, simply cannot gain access to the privately held evidence necessary to tie spam to a particular spammer. That is, the strong and admissible evidence by which a spammer can be identified and prosecuted is often in possession of a third-party (for example, a domain registrar, ISP, hosting company, on-line payment company or affiliate program operator) that is unwilling or unable to provide such information without compulsory process. Thus, the suppositions and inferences provided in leads, even if accurate, do not often add much value to the investigation and prosecution of spammers.

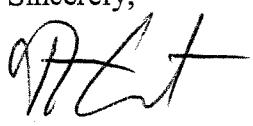
A reward system that encourages more leads may even be disruptive to effective enforcement. The investigation of each lead requires time, money and dedication. Internet service providers and law enforcement officials already spend a tremendous amount of time, resources and money pursuing available leads. As an ISP seeking to enforce the law against spammers, we hire outside investigators in an attempt to locate the sender of unlawful spam messages. We also work closely with our technology departments to identify elements of spam messages that may lead to the culprit. We share information with other ISPs to find those who have set up different e-mail accounts from which to send spam, and employ outside counsel to pursue spammers through litigation. Each lead investigation requires a significant investment, often many thousands of dollars, and not all such investigations lead to actionable targets. For example, Microsoft estimates that its internal team worked approximately 2,800 hours as part of its effort to identify spammers in 2003. Microsoft's U.S. outside legal and investigation team has included more than four attorneys, two paralegals, and several additional high-level technical investigators to handle the investigation and prosecution of spam targets. U.S. outside counsel and investigators worked more than 9,300 hours last year in their effort to analyze and trace persons responsible for spam. That combined effort led to an identification of 271 persons or entities responsible for spam (senders, beneficiaries, email marketers, affiliates and sub-affiliates), or approximately 45 hours per spammer. A reward system that created more leads would simply not alter the number of qualified targets that could be investigated.

CONCLUSION

In the end, we believe that reward programs, if specific and directed, can lead to the collection of important evidence that would otherwise not be obtained through diligent forensic work. However, even successful reward programs are only a component of the overall war against spam, and must be part of a more comprehensive enforcement program.

Microsoft appreciates the opportunity to provide these comments to assist the Commission with implementing the CAN-SPAM Act. We are committed to tackling spam on behalf of our customers and look forward to working with the Commission toward this common goal.

Sincerely,



Tim Cranton
Senior Attorney
Microsoft Corporation